

Is tornadocash.ws a scam? TrustSniffer's high-risk assessment: 0/100

tornadocash.ws

Verdict

0

OUT OF 100

CRITICAL RISK

tornadocash.ws shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

A hybrid site presenting itself as an educational Web3/Tornado Cash guide while simultaneously showing ecommerce product listings and clear gambling/deposit functionality (minimum deposits, withdrawals, jackpot/promotions, referral programs). The page lacks verifiable regulation/identity despite soliciting deposits and login, producing a high-risk profile.

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

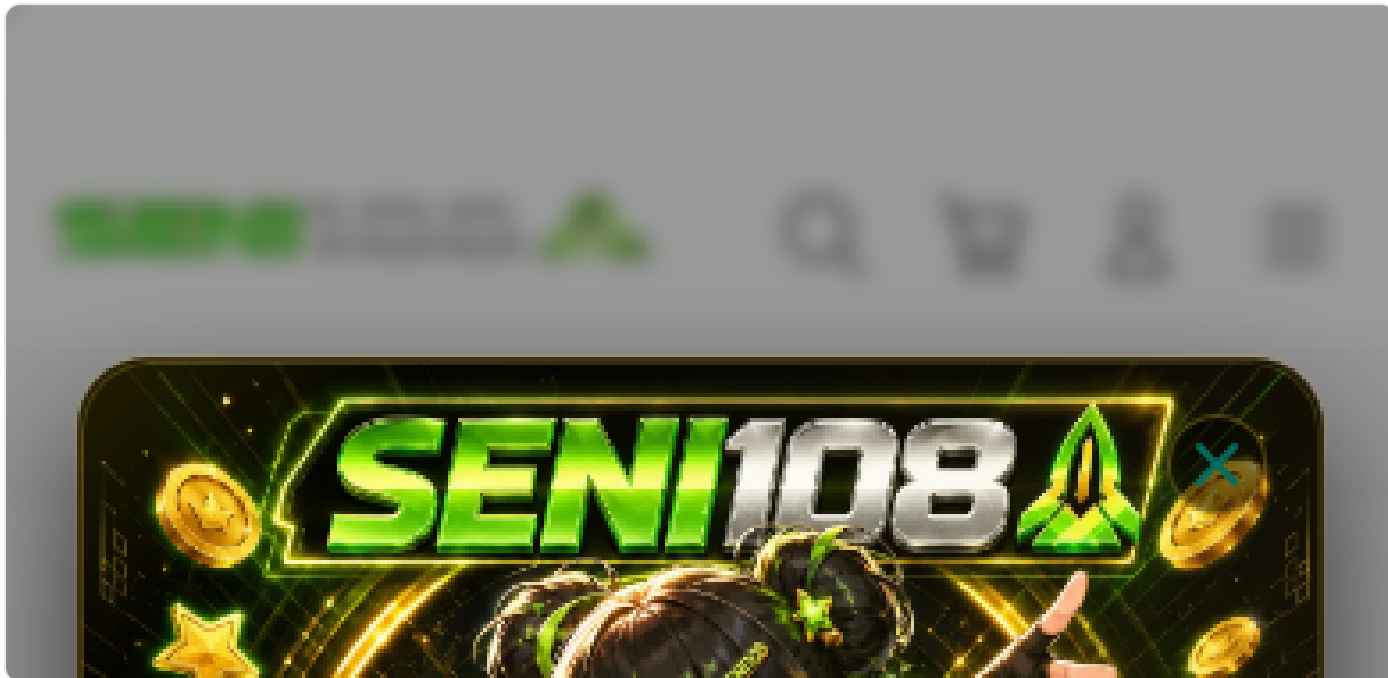
At a glance

The checks that decide most of this verdict.

Malware engines	15 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	1.8 years old Registered history	CLEAR
Web archive	Archived since 2024 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://tornadocash.ws/>



What tornadocash.ws served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2024.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Fortinet, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

This website presents itself as a hybrid educational Web3 and Tornado Cash guide, while also displaying Samsung-like ecommerce listings and deposit-based gambling functionality. Its apparent business model combines informational content and retail-style presentation with login, deposits, withdrawals, jackpots, promotions, and referral activity.

Scam/Impersonation Risk

Confirmed contradiction signals are present. External security intelligence recorded the domain as blacklisted, with 15 malicious and 3 suspicious detections, including detections from two enterprise security providers. The site's internal presentation is also materially inconsistent: an educational Tornado Cash and blockchain theme appears alongside ecommerce listings and gambling mechanisms involving minimum deposits, withdrawals, jackpots, promotions, and referrals. This combination creates an opaque value flow and a deposit-before-service risk, particularly because a sensitive login form solicits account interaction within the same mixed-content environment. No separate brand impersonation or conflicting legal-entity identity was

established, but the confirmed blacklist and malicious detections are sufficient to support a clearly cautionary assessment. Evidence:

- The homepage is titled “SENI108 – Panduan Lengkap (Tornadocash) Blockchain, Kripto, dan Teknologi Web3,” but also displays Samsung-like product categories, login prompts, deposit amounts, jackpots, and referral language.
- The homepage contains one sensitive form supporting login, sign-up, and deposit-action prompts.
- External reputation checks recorded 15 malicious detections, 3 suspicious detections, and a confirmed blacklist; Google Safe Browsing was negative.
- Historical continuity records the domain age as 1.75 years, with 35 snapshots across 2024–2026; the registration record lists creation on 2026-07-01 and an age of 0.14 years, creating a provenance inconsistency that should not be treated as evidence of established identity.

Regulatory Verification Notes

The site does not present a clearly verifiable operator identity, regulatory authority, or license number in the supplied page evidence. Its disclosure state is therefore unclear, which is a material transparency gap for a service soliciting deposits and presenting gambling-related functions. The available evidence does not establish that the site is licensed or regulated. A broker-reputation dataset produced no match, but that absence is contextual only and does not validate the operator or its activities. Evidence:

- The homepage and visible navigation expose login, sign-up, deposit, withdrawal, jackpot, and referral functions without a stated licensing authority or license number.
- The site's independently verified identity status is unverified.
- Served from AS13335 (CLOUDFLARENET – Cloudflare, Inc., US).
- TLS certificate issued by WE1 with DV validation, valid to 2026-11-17.

What to Verify Next

Before any sensitive interaction, an independent review should identify the real-world operator and confirm any applicable gambling, financial, or payments authorization directly with the relevant regulator. Payment ownership, withdrawal conditions, dispute mechanisms, and the authenticity of official support channels should be confirmed through independent contact routes rather than links or details supplied solely by the site. Existing credentials should not be reused on this domain, and any payment or account activity should be reviewed for unauthorized changes.

EVIDENCE

- Identity verification is currently unverified, so the site's on-page branding cannot establish the operator's real-world identity.
- The on-page regulatory disclosure state is unclear.
- External reputation evidence includes a confirmed blacklist and malicious detections, requiring independent validation before interaction.

Summary Verdict

The overall posture is **critical risk**, driven by corroborated external threat detections and a materially inconsistent operating presentation. The available evidence does not support treating the website as a trustworthy destination for sensitive, credential-based, or financial activity.

Infrastructure Integrity

The website is protected by Cloudflare CDN/WAF infrastructure, with observed Cloudflare edge addresses and a potential origin candidate. This provides a degree of network-layer exposure mitigation, but protective hosting infrastructure is not evidence of operator legitimacy and cannot offset the site's external reputation findings.

Closing Assessment

Engagement should be suspended for login, credential submission, deposits, payments, or other sensitive activity unless the operator's identity, authorization, and transaction safeguards are independently established and the external security findings are resolved.

Written analysis generated 2026-08-21 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, behaviour in a sandbox, external reputation.

01 Governance Risk

- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.

Registration and ownership rule:KF_WHOIS_PRIVATE

- The registration record withholds contact details for the operator.

Registration and ownership rule:KF_WHOIS_HIDDEN

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.

Analysis engine signal:direct_threat

- The structure of the page changed sharply while it was loading.

Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE

- Most of what the page loaded came from other domains rather than from this one.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH

- The page replaced a large part of its own content after loading.

Behaviour in a sandbox rule:BEHAV_DOM_CHANGE_HIGH

- The page rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.

Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION

- The page sent data to a destination TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS

- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.

External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	25%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of tornadocash.ws.

- The request stayed on tornadocash.ws. It was not redirected to another domain. CLEAR
- Registration is published under NAMECHEAP INC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-07-01. NOTED
- The earliest public archive of this site is from 2024-11-19. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NAMECHEAP INC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3036::ac43:cad4
Name servers	dane.ns.cloudflare.com, gabriella.ns.cloudflare.com
SSL issuer	WE1
SSL expiry	2026-11-17
Domain age	1.75 years (continuous registration)
Domain expiry	2027-07-01
Archive first seen	2024-11-19
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 15 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about tornadocash.ws at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/tornadocash.ws> · assessed 2026-08-21